IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

CHARLES METZGER, individually and on behalf of all others similarly situated, Plaintiff, v. **COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY,** and **CITRIX SYSTEMS, INC.**, Defendants.	Case No. Judge **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Charles Metzger ("Plaintiff") brings this action individually, and on behalf of all others similarly situated, by and through counsel, against Defendants Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast"), and Citrix Systems, Inc. ("Citrix") (collectively, "Defendants"), for their failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") stored within Defendants' information network.

Plaintiff makes these allegations on personal information as to those allegations pertaining to himself and his personal circumstances, and upon information and belief, based on the investigation of counsel and facts that are matters publicly known, on all other matters.

INTRODUCTION

1. Plaintiff brings this action on behalf of himself and all other individuals similarly situated ("Class Members") against Comcast and Citrix for their failure to secure and safeguard the PII of at least 35 million customers that was maintained on Defendants' computer systems, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII (the "Data Breach").[1]

2. On or about October 10, 2023, Citrix alerted Comcast to a vulnerability in one of its products used by Comcast. That same day, Citrix issued a patch to fix the vulnerability.

3. Despite knowledge of the vulnerability, Comcast did not patch its network until October 16, 2023 at the earliest, and October 19, 2023 at the latest—a lapse of six to nine days.

4. On or before November 16, 2023, Comcast was made aware that an unauthorized third party gained access to its internal computer network systems as a result of the vulnerability and absconded with computer files containing the PII of nearly all of its 35 million customers.

5. Comcast, headquartered in Philadelphia, Pennsylvania, is one of the largest internet providers in the United States. In the regular course of its business,

[1] https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited, January 8, 2024)

Comcast is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosures.

6. Comcast uses Citrix, a cloud computing company, for cloud computing and virtualization services, which requires Comcast to transfer Plaintiff's and Class Members' PII to Citrix.

7. Defendants' customers, like Plaintiff and Class Members, provided certain PII to Defendants, which is necessary to obtain Defendants' services.

8. Large companies like Defendants have an acute interest in maintaining the confidentiality of the PII entrusted to them, and they are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding PII in their possession.

9. Plaintiff and Class Members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information as part of obtaining internet services. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

10. Despite the dire warnings about the severe impact of data breaches on

Americans of all economic strata, Defendants still failed to make the necessary investments to implement important and adequate security measures to protect their customers' data.

11. Defendants required customers to provide their sensitive PII and failed to protect it. Defendants had an obligation to secure customers' PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff and Class Members and Defendants.

12. As a result of Defendants' failure to provide reasonable and adequate data security, Plaintiff and the Class Members' unencrypted, non-redacted PII has been stolen by criminals who intend to use it to commit fraud. Plaintiff and Class Members are now at a significant risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII in Defendants' possession, including personally identifiable information, internet activity, financial information, and billing information. This risk constitutes a concrete injury suffered by Plaintiff and Class Members, and they no longer have control over their PII.

13. Furthermore, Plaintiff and Class Members have and will have to continue to pay for credit monitoring and identity theft protection services for the foreseeable future as a direct result of the Data Breach.

14. Plaintiff brings this action on behalf of himself and those similarly situated to seek redress for the harm they have suffered and will continue to suffer,

including, but not limited to reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Defendants to ensure that their third-party vendors implement and maintain reasonable data security practices going forward.

JURISDICTION & VENUE

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because there are 100 or more members of the proposed class, at least one Class Member has diverse citizenship from at least one Defendant, and the amount in controversy exceeds $5,000,000, exclusive of costs.

16. Venue lies in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

THE PARTIES

Plaintiff Charles Metzger

17. Plaintiff is a citizen and resident of Ohio.

18. In the course of using Comcast's services, Plaintiff was required to provide his PII to Defendant, including his name, social security number, date of birth, address, and contact information.

19. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach. Plaintiff received a Notice of Data Breach on January 4, 2024 via an email from Comcast.

20. At all times herein relevant, Plaintiff is and was a member of the Class.

21. As a result of the Data Breach, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny; time spent dealing with increased spam emails; and time spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach.

22. Plaintiff was also injured by the material risk to future harm he suffers based on the Defendants' Data Breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the Data Breach, and the data involved is highly sensitive and presents a high risk of identity theft or fraud.

23. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII that he entrusted to Defendants, and which was compromised in and as a result of the Data Breach.

24. Plaintiff, as a result of the Data Breach, has increased anxiety about his loss of privacy and anxiety over the impact of cybercriminals accessing, using, and

selling his PII.

25. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

26. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in the Defendants' possession, is protected and safeguarded from future breaches.

Defendant Comcast Cable Communications, LLC d/b/a Xfinity

27. Comcast has its principal place of business in Philadelphia, Pennsylvania and is organized in Delaware.

28. Comcast advertises itself as a global media and technology company that reaches hundreds of millions of customers worldwide.[2]

29. Through its Xfinity platform, Comcast prides itself on being the largest internet provider in the United States.[3]

30. The true names and capacities of persons or entities, whether

[2] https://corporate.comcast.com/company (last visited, January 8, 2024)
[3] https://corporate.comcast.com/company/connectivity-platforms (last visited, January 8, 2024)

individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

31. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

Defendant Citrix Systems, Inc.

32. Citrix is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida.

33. Citrix provides cloud computing and virtualization services throughout the United States.

34. Comcast uses Citrix services, which requires Comcast to transfer Plaintiff's and Class Members' PII to Citrix.

35. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

36. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

STATEMENT OF FACTS

Defendants' Data Breach

37. On or about October 10, 2023, Citrix notified Comcast of a vulnerability in its network hardware and issued a patch that same day. Despite knowledge of the vulnerability, Comcast did not patch its network until October 16, 2023 at the earliest, and October 19, 2023 at the latest—a lapse of six to nine days.

38. It was later discovered that prior to Comcast's mitigation efforts, an unauthorized party accessed Comcast systems sometime between October 16, 2023 through October 19, 2023, obtaining highly sensitive PII of its customers including first and last names, Social Security numbers, dates of birth, addresses, and contact information.

39. Based on Comcast's concession that the unauthorized access occurred between at least October 16, 2023 and October 19, 2023, it is reasonable to conclude that the criminals were able to gain access undetected and unimpeded for long enough to satisfy themselves that they had extracted all sensitive and valuable information from Comcasts' systems.

40. In January 2024, Comcast issued a Data Breach Notice (the "Notice") to notify its customers of the Data Breach.

41. Plaintiff received an email notifying him of the Data Breach on January 4, 2024. *See* **Exhibit 1** - Data Breach Notice.

42. The Notice advises Plaintiff and Class Members that "To protect your account, we have proactively asked you to reset your password. The next time you

login to your Xfinity account, you will be prompted to change your password, if you haven't been asked to do so already." The Notice further encourages customers "to enroll in two-factor or multi-factor authentication."

43. Comcast attempts to assure its customers that "we remain committed to continue investing in technology, protocols and experts dedicated to helping to protect your data and keeping you, our customer, safe" but offers no third-party credit monitoring or theft protection services to actually assist customers in the protection and safety of their highly sensitive data.

44. Instead, Comcast advises customers to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."

Defendants Collected/Stored Class Members' PII

45. Defendants acquired, collected, stored, and assured reasonable security over Plaintiff's and Class Members' PII.

46. As a condition of their relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly sensitive and confidential PII.

47. Defendants, in turn, stored that information in the part of Defendants' computer and information system that was ultimately affected by the Data Breach.

48. By obtaining, collecting, and storing Plaintiff's and Class Members'

PII, Defendants assumed legal and equitable duties to protect that PII and knew or should have known that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

49. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

50. Plaintiff and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized use of this information.

51. Defendants represented to consumers and the public that they possess robust security features to protect PII and that they take their responsibility to protect Private Information seriously

52. Comcast's privacy policy states:

> Your privacy matters to us
>
> We know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it.[4]
>
> We follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices include technical, administrative, and physical safeguards, which may vary, depending on the type and

[4] https://www.xfinity.com/privacy (last visited, January 9, 2024)

sensitivity of the information.[5]

53. Citrix's privacy policy states:

> Cloud Software Group, Inc. and its subsidiaries ("Cloud Software Group"), respect your concerns about privacy.
>
> We maintain administrative, technical and physical safeguards, consistent with legal requirements where the personal information was obtained, designed to protect against unlawful or unauthorized destruction, loss, alteration, use or disclosure of, or access to, the personal information provided to us through the Channels.[6]

54. Citrix further states in its Data Processing Addendum:

> We shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such security practices are set forth in the Cloud SG Security Exhibit, which is available at https://www.cloud.com/trustcenter/citrix-services-security-exhibit. We seek to continually strengthen and improve its security practices, and so reserve the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of Products and/or Services. Our employees are bound by appropriate confidentiality agreements and required to take regular data protection training as well as comply with Our corporate privacy and security policies and procedures.[7]

55. Defendants could have prevented the Data Breach, which began no later than October 10, 2023, by adequately securing and encrypting and/or more securely

[5] *Id.*
[6] https://www.cloud.com/privacy-policy (last visited January 9, 2024)
[7] https://www.cloud.com/content/dam/cloud/documents/legal/cloud-software-group-data-processing-addendum-oct-2023.pdf (last visited Jan. 9, 2024)

encrypting their servers generally, as well as Plaintiff's and Class Members' PII.

56. Defendants' negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings, and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

57. Yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

58. Defendants' failure to adequately secure Plaintiff's and Class Members' sensitive PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

59. In 2022, 1,802 data breaches occurred, resulting in over 422,000,000 sensitive records being exposed.[8] The over 422,000,000 records being exposed in 2022 represents a substantial increase from 2021 when 293,927,708 sensitive

[8] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited January 9, 2024)

records were exposed in 1,862 data breaches.[9]

60. In light of recent high profile data breaches at other industry leading companies, including MOVEIt (17.5 Million Records, June 2023), LastPass/GoTo Technologies (30 Million Records, August 2022), Neopets (69 Million Records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 Million records, July 2022), Cash App (8.2 Million Users, April 2022), LinkedIn (700 Million Records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

61. Moreover, Defendants were, or should have been, aware of the foreseeable risk of a cyberattack, like the one it experienced. In fact, Okta published a warning directly warning of this type of attack in 2011.

62. The Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or

[9] *Id.; see also* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6. (last visited, January 9, 2024)

practices in or affecting commerce."[10]

63. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

64. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and their vendors', networks, and protocols adequately protected the PII of Plaintiff and Class Members.

65. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their and their vendors' computer systems, servers, networks, and personnel policies and procedures to ensure that the PII was adequately secured and protected.

66. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

[10] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

67. Defendants owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in their data security systems in a timely manner.

68. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

69. Defendants owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

70. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

71. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

72. PII are valuable commodities for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

73. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information is sold at prices ranging from $40 to $200, and

bank details have a price range of $50 to $200.[11] Criminals also can purchase access to entire sets of information obtained from company data breaches for prices ranging from $900 to $4,500.[12]

74. Social Security numbers are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

75. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

76. In addition, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive

[11] Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-onthe-dark-web-how-much-it-costs/ (Last visited January 9, 2024).

[12] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark (Last visited January 9, 2024).

[13] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (Last visited January 9, 2024).

action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[14]

77. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

78. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, and Social Security number.

79. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security

[14] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-shackers-has-millionsworrying-about-identity-theft (Last visited January 9, 2024).

numbers are worth more than 10x on the black market."[15]

80. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

81. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

82. Here, Defendants knew of the importance of safeguarding PII and of

[15] Time Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10xprice-of-stolen-credit-card-numbers.html (Last visited January 9, 2024)

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 9, 2024).

the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

83. Defendants are large, sophisticated organizations with the resources to deploy robust cybersecurity protocols. They knew or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiff and Class Members. Therefore, their failure to do so is intentional, willful, reckless and/or grossly negligent.

84. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

Common Injuries & Damages Suffered by the Plaintiff and Putative Class

85. As a result of Defendants' ineffective and inadequate data security

practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is present and continuing, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

86. Plaintiff and Class Members are at a heightened risk of identity theft for years to come. The link between a data breach and the risk of identity theft is simple and well-established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes discussed below.

87. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise

mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

88. Plaintiff and Class Members have spent and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

89. These efforts are consistent with the U.S. Government Accountability Office report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

90. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

[17] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report"). (last visited January 9, 2024)
[18] *Id.*

91. The value of the PII of the Plaintiff and Class Members is valuable.[19] Its value is axiomatic, considering the value of Big Data in corporate America and the criminal consequences of cyber thefts, which include significant prison sentences and fines. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has a considerable market value.

92. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[20]

93. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

94. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

[19] See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (Last visited January 9, 2024).

[20] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited January 9, 2024).

95. There is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

96. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. And fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

97. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

CLASS ACTION ALLEGATIONS

98. Plaintiff, individually and on behalf of others similarly situated, seeks to certify the following class of similarly situated persons under Rule 23 of the Federal Rules of Civil Procedure:

> All persons whose PII was maintained on Defendants' servers that were compromised in the Data Breach.

99. Excluded from the Class are Defendants' officers and directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their immediate families and members of their staff.

100. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

101. **Numerosity.** A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class (which Plaintiff is informed and believe, and on that basis, alleges that the total number of persons exceeds 35 million are so numerous that joinder of all members is impractical, if not impossible.

102. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether the Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendants actually learned of the Data Breach;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their

systems, resulting in the loss of the PII of Plaintiff and Class Members;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendants' wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

103. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

104. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel is competent and experienced in litigating class actions.

105. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' PII was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

106. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

107. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(On behalf of Plaintiff and the Class against all Defendants)

108. Plaintiff realleges paragraphs 1–107 as if fully set forth herein.

109. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PII of Plaintiff and Class Members in their computer systems and on their networks.

110. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

111. Defendants knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

112. Defendants knew or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of their data security systems, and the importance of adequate security.

113. Defendants knew about numerous, well-publicized data breaches.

114. Defendants knew or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

115. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

116. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

117. Because Defendants knew that a breach of their systems could damage millions of individuals, including Plaintiff's and Class Members, Defendants had a duty to adequately protect their data systems and the PII contained therein.

118. Plaintiff's and Class Members' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions.

119. Moreover, only Defendants had the ability to protect their systems and the PII it stored on them from attack. Thus, Defendants had a special relationship with Plaintiff and Class Members.

120. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants, Plaintiff, and/or the remaining Class Members.

121. Defendants breached their general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and

Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train their employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

122. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

123. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

124. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continue to breach their disclosure obligations to Plaintiff and Class Members.

125. Further, through their failure to provide clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

126. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

127. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

128. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

129. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

130. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

131. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

COUNT II
Negligent Misrepresentation
(On behalf of Plaintiff and the Class against all Defendants)

133. Plaintiff realleges paragraphs 1–132 as if fully set forth herein.

134. Defendants supplied false information for the guidance of others in the course of their business. As alleged above, Defendants falsely represented that their superior data security practices would protect Plaintiff and Class Members from the Data Breach, when in actuality, Defendants employed deficient and unreasonable data security practices.

135. Defendants' representations were false and Defendants failed to exercise reasonable care in obtaining or communicating the information. Defendants' data security practices were unreasonable and deficient by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class Members' PII;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and other Class Members' PII;

d. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiff's and other Class Members' PII;

e. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiff's and other Class Members' PII reasonably and appropriately in order to repel or limit the Data Breach;

f. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained for legitimate and useful purposes;

g. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiff's and other Class Members' PII;

h. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

i. Failing to provide full disclosure, deceptively misleading customers through false representations and misleading omissions of fact regarding the Data Breach, customers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

j. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and other Class Members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the

disposition of Plaintiff's and other Class Members' PII at all times during the Data Breach.

136. Plaintiff and Class Members justifiably relied on Defendants' false information and were induced to obtain Defendants' products and services in reliance thereon.

137. As a direct and proximate result of Defendants' numerous negligent acts and omissions, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the Data Breach, including the instructions in the Data Breach Letter; (e) the cost of future monitoring for identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

138. As a direct and proximate result of Defendants' negligent misrepresentation, Plaintiff and Class Members are entitled to recover actual and punitive damages.

COUNT III
Breach of Implied Contract

(On behalf of Plaintiff and the Class against all Defendants)

139. Plaintiff realleges paragraphs 1–138 as if fully set forth herein.

140. Defendants required Plaintiff and Class Members to provide their PII as a condition of receiving internet services. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants wherein Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their PII had been breached and compromised or stolen.

141. Defendants further entered into an implied contract with Plaintiff and the Class Members to honor their representations and assurances regarding protecting their PII.

142. Plaintiff and Class Members fully performed their obligations under implied contracts with Defendants.

143. Defendants, through their own actions and omissions breached the implied contracts it made with Plaintiff and Class Members by (i) failing to implement technical, administrative, and physical security measures to protect the PII from unauthorized access or disclosure, despite such measures being readily available, (ii) failing to limit access to the PII to those with legitimate reasons to access it, (iii) failing to store the PII only on servers kept in a secure, restricted area, and (iv) otherwise failing to safeguard the PII.

144. As a direct and proximate result of Defendants' breach of their implied contract, Plaintiff and Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

145. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) financial costs incurred due to actual identity theft; (d) the cost of future identity theft monitoring; (e) loss of time incurred due to actual identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

146. As a direct and proximate result of the above-described breaches of implied contract, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Breach of Third-Party Beneficiary Contract
(On behalf of Plaintiff and the Class against Citrix)

147. Plaintiff realleges paragraphs 1–146 as if fully set forth herein.

148. Citrix entered into contracts with its clients, including Comcast, to provide cloud computing and virtualization services.

149. Citrix's services included data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to it.

150. Such contracts were made expressly for the benefit of Plaintiff and Class Members, as it was their PII that Citrix agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and Class Members was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

151. Citrix knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

152. Citrix breached its contracts with customers by, among other things, failing to adequately secure Plaintiff and Class Members' PII, and, as a result, Plaintiff and Class Members were harmed by Citrix's failure to secure their PIII.

153. As a direct and proximate result of Citrix's breach, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft;

(c) financial costs incurred due to actual identity theft; (d) the cost of future identity theft monitoring; (e) loss of time incurred due to actual identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

154. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach

COUNT V
Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiff and the Class against all Defendants)

155. Plaintiff realleges paragraphs 1–154 as if fully set forth herein.

156. Plaintiff and Class Members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

157. Defendants intruded upon that seclusion by allowing the unauthorized access to the Plaintiff and Class Members' PII without Plaintiff and Class Members' consent, knowledge, authorization, notice, or privilege by negligently maintaining the confidentiality of Plaintiff and Class Members' information as set out above.

158. Defendants' breach of confidentiality resulted in insecure systems allowing harmful disclosure of the information to criminals and criminal data markets.

159. The intrusion was offensive and objectionable to Plaintiff, the Class Members and to a reasonable person or ordinary sensibilities in that Plaintiff and Class Members' PII was disclosed without prior written authorization of Plaintiff and the Class.

160. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class Members provided and disclosed their PII to Defendants privately with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without consent. Plaintiff and the Class Members were further reasonable to believe that the PII would be reasonably protected against third-party criminal extraction through foreseeable hacking activity.

161. This improper disclosure increased the risk that the personal data was delivered to criminal data markets thereby increasing the risk of identity theft to Plaintiff and the Class Members.

162. As a direct and proximate result of Defendants' unauthorized disclosure, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and

loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the Data Breach, including the instructions in the Data Breach Letter; (e) the cost of future monitoring for identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

163. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach

COUNT VI
Unjust Enrichment
(On behalf of Plaintiff and the Class against all Defendants)

164. Plaintiff realleges paragraphs 1–107 as if fully set forth herein.

165. This claim is brought in the alternative.

166. Defendants benefited from receiving Plaintiff's and Class Members' PII by their ability to retain and use that information for their own benefit.

167. Defendants also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

168. Plaintiff and Class Members conferred a benefit upon Defendants by paying for services, and in connection therewith, by providing their PII to Defendants with the understanding that Defendants would implement and maintain

reasonable data privacy and security practices and procedures. Plaintiff and Class Members should have received adequate protection and data security for such PII held by Defendants.

169. Defendants knew Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and appreciated the benefits.

170. Defendants failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

171. Defendants should not be permitted to retain money rightfully belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data security measures and caused the Data Breach.

172. Defendants accepted and wrongfully retained these benefits to the detriment of Plaintiff and Class Members.

173. Defendants' enrichment at the expense of Plaintiff and Class Members is and was unjust.

174. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and Class Members seek restitution of their money paid to Defendants, and disgorgement of all profits, benefits, imposition of a constructive trust, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment against Defendants and in Plaintiff's favor, as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

e) For an award of punitive damages, as allowable by law;

f) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

g) Pre- and post-judgment interest on any amounts awarded; and,

h) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 19, 2024

Respectfully Submitted,

s/William Wright
The Wright Law Office, P.A.
515 N. Flagler Drive P300
West Palm Beach, FL 33401
willwright@wrightlawoffice.com
561-514-0904

Marc E. Dann*
Brian D. Flick*
**Pro Hac Vice Application*

Anticipated

DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
**Pro Hac Vice Application*
Anticipated

ZIMMERMAN LAW OFFICES, P.C.

77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com

Attorneys for Plaintiff and the proposed Class